(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2001 (02.08.2001)

PCT

(10) International Publication Number
WO 01/55979 A1

(51) International Patent Classification[7]: G07F 7/10 // G06F 17/60

(21) International Application Number: PCT/FI01/00063

(22) International Filing Date: 24 January 2001 (24.01.2001)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20000135 24 January 2000 (24.01.2000) FI

(71) Applicant *(for all designated States except US)*: SONERA SMARTTRUST OY [FI/FI]; c/o Sonera Oyj, P.O. Box 106, FIN-00051 Sonera (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: BLUMENTHAL, Henrik [FI/FI]; Sonera SmartTrust Oy, P.O. Box 425, FIN-00051 Sonera (FI).

(74) Agent: PAPULA OY; P.O. Box 981 (Fredrikinkatu 61 A), FIN-00101 Helsinki (FI).

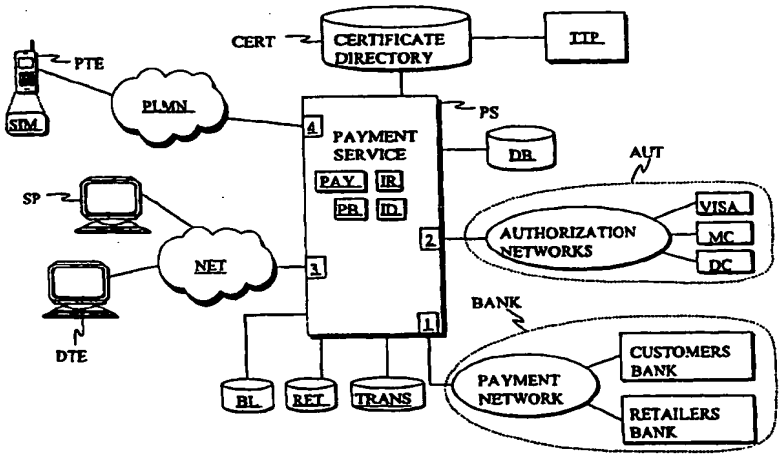
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PAYMENT DEVICE AND METHOD FOR SECURE PAYMENT



(57) Abstract: The present invention relates to the implementation of data secure payments services and devices. In particular, the present invention relates to payment service equipment (PS) and to two methods in which payment service equipment (PS) is used. Thanks to the present invention, the paying with a payment card may be implemented via an information network such as the Internet in such a way that the paying is secure and that the number of the client's payment card does not need to be transmitted over the data transmission network. In the invention, the client is requested for a separate confirmation for effecting the payment. The piece of information to be confirmed is sent to the terminal device of the client, preferably a mobile station, by means of which the client digitally confirms the order made by him or her by signaling the confirmation received. The signed confirmation as well as the electronic identity information associated with the client is sent back to the payment service equipment (PS). The payment service equipment (PS) takes care of the verifying of the client's identity, of the checking of the validity of the client's payment card and of the eventual transmitting of the payment information to the payment system (BANK).

WO 01/55979 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Payment device and method for secure payment

FIELD OF THE INVENTION

The present invention relates to telecommunication systems. In particular, the invention relates to payment service equipment and method by means of which the security of use of a payment card, especially a credit card, may be improved.

BACKGROUND OF THE INVENTION

In a traditional payment transaction, the client visits the offices of a merchant, chooses the desired products from the shelves and eventually pays his/her purchases, e.g. in cash or with a bank or credit card. Besides the traditional commerce there is the purchasing and paying of trade or different services via different telecommunication networks. In a mobile communication network, e.g. in the GSM system (GSM, Global System for Mobile communications), it is possible to make and pay different purchases with the mobile station. In addition, the mobile station may be used to digitally sign and/or encrypt outgoing traffic for different operating applications. This practice helps to improve the data security in measures requiring it. In encryption and signing, a so-called public key infrastructure is often used (PKI, Public Key Infrastructure).

In the public key infrastructure, the user has got two keys, a public key and a private key. If the user wishes to send encrypted information to somebody, then he or she encrypts the information with the recipient´s public key. The information encrypted with the public key may be transformed into a readable form only with a private key associated with the public key. The digital signature is used to mean a way of action in which one acts exactly contrary to the encryption of the message. The sender signs the message

with his or her own private signing key and the recipient may in turn decode the message into a readable form with the sender´s public signing key. This is to make sure that the sender really is the person he or she claims to be.

The paying via the Internet has been possible for a long time. The general practice is that the client visits the www sites (WWW, World Wide Web) of a merchant or other service provider, chooses the desired products and effects the payment for the chosen products. One possibility of effecting the payment is to transmit the credit card number directly to the merchant over the Internet without any encryption operations at all. This alternative, does not, however, take any stand on the security of the effecting of the payment.

On the whole, there are several electronic payment modes differing from one another developed in conjunction with the Internet. Examples of these are, for instance, Ecash, solo of the Merita Bank, Kultaraha of the bank Osuuspankki and the SET (SET, Secure Electronic Transaction) of credit card companies. SET is an international payment system developed together by VISA and MasterCard for secure purchasing on the Internet. SET is based on certificates issued by a trusted third party and on encrypted transmission of information. SET uses a symmetric and asymmetric encryption, digital signature as well as a SHA-1 algorithm (SHA, Secure Hash Algorithm). The SET standard aims at the encryption of information, confidentiality, checking of the integrity of the information, authentication of the sender and indisputability.

The symmetric encryption is used to mean an encryption method in which the encrypted message may be decoded with the same key as the message was encrypted. One example of this kind of method is DES (DES, Data Encryption Standard). The asymmetric en-

cryption is used to mean that the message is encrypted and decoded using different keys. One example of this kind of method is the public key method RSA (RSA, Rivest, Shamir, Adleman).

In the present practices of purchasing on the Internet there are several problem points. The systems supporting the cards are often card-specific. The same applications cannot be used for paying with a credit card issued by another company. Therefore, the commercial centres have to support the payment practice of several different systems.

In order that the security of paying with a credit card can be improved, all the parties associated with the payment transaction - both the client and the merchant - have to often make investments in reliable software. If the investments required are too high, then this for its part is an obstacle to the spreading of commerce in the network.

There are methods in which both of the parties of the commerce, the client and the merchant, have got their own certificates. The certificate is used to mean a kind of identification information issued by a trusted third party (TTP, Trusted Third Party). In the case of a credit card payment, the meaning of the certificate is that it indicates that the user has got a credit card valid for paying. A certificate issued to the merchant gives in turn proof of the fact that the merchant is an authorized merchant. By means of certificates, both the client and the merchant can make sure of the identity of one another. The use of certificates, digital signature and encryption remarkably adds to the security of paying with the credit card on the Internet.

The known modes of credit card payments have, however, weak points. The complexity of the payment system and the heavy investments were already discussed above. The biggest problem is, however, the

fact that the credit card number of the client is sent over the data transmission network. Furthermore, some known methods require the use of a so-called digital wallet (Digital Wallet). The digital wallet includes client-specific information, e.g. the certificate of the client, credit card number, the validity of the card, etc. The requirement for a successful payment transaction is that the digital wallet is in the terminal device by means of which the client is making the purchase.

OBJECTIVE OF THE INVENTION

The objective of the invention is to eliminate the drawbacks referred to above or at least significantly to alleviate them. One specific objective of the invention is to disclose a new type of payment service equipment and method which enable one to securely pay with a payment card, especially with a credit card, in an information network such as the Internet. The credit card number of the client is not sent over the data transmission network at all. In addition, the method in accordance with the invention does not take any stand on the fact who has issued the payment card, instead the method functions regardless of the card.

BRIEF DESCRIPTION OF THE INVENTION

The invention relates to the improvement of the security of a payment transaction effected with a payment card via the Internet. The payment service equipment and method in accordance with the invention enable the fact that the client may pay the products or services desired by him or her with his or her payment card via the Internet without having to send his or her credit card number over the telecommunication network at all. In addition, the method in accordance

with the invention is in no way bound to the use of a payment card issued by a particular computer or company.

The payment service equipment in accordance with the invention comprises a first access interface to the payment system, a second access interface to the authentication system and a third access interface to the telecommunication network. The payment service equipment further comprises a certificate database for saving the certificates associated with the clients, a service provider database for saving information relating to the registered service providers, a client database for saving information relating to the clients, a transaction database for saving information relating to the payment transactions and a verification database which includes an auxiliary list of suspicious payment cards.

According to the invention, the client database comprises, e.g. the mobile number of the client and information relating to the payment card of the client. The payment card of the client is advantageously used to mean a credit card. The payment card information of the client may be included also as a part of the certificate associated with the client. The payment service equipment further comprises a generation block for generating the billing ticket connected with the payment transaction, a telecommunication block for sending and receiving the confirmation of purchase connected with the billing ticket, an identification block for identifying the client based on the electronic identity and signature, and an information retrieval block for checking the credit card information of the client.

It is possible to encrypt the information included in the client database and service provider database, e.g. using a public key of the service payment equipment.

In an embodiment of the invention, the service payment equipment comprises a fourth access interface to the mobile communication network.

The present invention also relates to a method for secure paying in a telecommunication system comprising a mobile communication network, a telecommunication network, a payment terminal device which comprises a smart card and which is connected to the mobile communication network or to the telecommunication network, a trusted third party, a payment system, service provider and an authentication system. In the method, a certificate associated with the client is generated and issued by the trusted third party, the product or service to be ordered is chosen via the service provider by means of a display terminal device via the telecommunication and/or mobile communication network and the client's payment card and/or payment card information is used for the paying of the product or service ordered.

According to the invention, the payment service equipment is used to generate a billing ticket. A confirmation of order is sent to the payment terminal device of the client via the mobile communication network. The payment terminal device is advantageously used to mean a mobile station. The smart card is advantageously used to mean a subscriber identity module (SIM, Subscriber Identity Module) inserted into the mobile station. The aforementioned confirmation of order is signed and/or encrypted in the payment terminal device. The signature and/or encryption is carried out by means of a smart card. Stored on the smart card are the necessary keys for carrying out the signing and/or encryption. Stored on the smart card is preferably the electronic identity of the client, the private key associated with the client and the public key associated with the payment service equipment.

The signed and/or encrypted confirmation of order and the electronic identity associated with the client are sent from the payment terminal device to the payment service equipment via the mobile communication network. The client is identified by the payment service equipment based on the electronic identity. The client is identified, e.g. based on the information included in the certificate database. The payment card number associated with the client is retrieved and the use of right of the payment card is verified. The payment is accepted, if the verification of the payment card was successful. Prior to accepting the payment one may check in the verification database attached to the payment service equipment that the client´s payment card is not among suspicious or forbidden payment cards. The request for the debiting of the payment is sent further to be implemented in the payment system.

The validity of the payment card is checked, e.g. in a separate authentication system. The payment card information associated with the client is retrieved, e.g. from the database of the payment service equipment. In an embodiment of the invention, the payment card number of the client is retrieved from a certificate database attached to the payment service equipment. The payment card is advantageously used to mean a Visa, MasterCard or Diners Club card or a bank card.

When the use of the client´s payment card has been accepted, the service provider may be sent a confirmation of the fact that the payment associated with the order has been effected. A similar confirmation may also be sent to the display terminal device or payment terminal device of the client.

In an embodiment of the invention, the payment terminal device and display terminal device are

used to mean a mobile station which comprises both facilities.

In an embodiment of the invention, the payment terminal device is used to mean a mobile station and the display terminal device a computer.

In an embodiment of the invention, the trusted third party updates the certificate database. The trusted third party is used to mean, e.g. a certificate authority (CA, Certificate Authority).

In an embodiment of the invention, the mobile communication network is used to mean a mobile communication network consistent with the GSM system.

In an embodiment of the invention, the telecommunication network is used to mean a packet-switched network, e.g. an Internet network.

The present invention also relates to a method for secure paying in a telecommunication system comprising a telecommunication network, a terminal device into which there is a card reader inserted and into which card reader it is possible to input a smart card and which terminal device is connected to the telecommunication network, a trusted third party, a payment system, a service provider and an authentication system. In the method, the trusted third party generates and issues the certificate associated with the client, the product or service to be ordered is chosen from the service provider by means of the terminal device via the telecommunication network, and the client´s payment card and/ or payment card information is used for paying the ordered product or service.

According to the invention, the payment service equipment is used to generate a billing ticket. A confirmation of the order that was made is sent to the terminal device of the client via the telecommunication network. The terminal device is advantageously used to mean a computer. The confirmation of order is

signed and/or encrypted by means of the terminal device. The signing and/or encryption is enabled by means of a card reader attached to the terminal device and by means of a smart card inserted into it. The client inputs into the card reader his or her own smart card on which there are the necessary keys stored for carrying out the signing and/or encryption. Stored on the smart card is preferably the electronic identity of the client, the private key associated with the client and the public key associated with the payment service equipment.

The signed and/or encrypted confirmation of order and the electronic identity associated with the client are sent from the payment terminal device to the payment service equipment via the telecommunication network. The client is identified by the payment service equipment based on the signature and/or electronic identity. The client is identified, e.g. based on the information included in the certificate database. The payment card number associated with the client is retrieved and the use of right of the payment card is verified. The payment is accepted, if the verification of the payment card was successful. Prior to accepting the payment one may check in the verification database attached to the payment service equipment that the clien´ts payment card is not among suspicious or forbidden payment cards. The request for the debiting of the payment is sent further to be implemented in the payment system.

The validity of the payment card is advantageously checked in a separate authentication system. The payment card information associated with the client is retrieved, e.g. from the database of the payment service equipment. In an embodiment of the invention, the payment card number of the client is retrieved from the certificate database attached to the payment service equipment. The payment card is advan-

tageously used to mean a Visa, MasterCard or Diners Club card or a bank card.

When the use of the client's payment card has been accepted, the service provider may be sent a confirmation of the fact that the payment associated with the order has been effected. A similar confirmation may also be sent to the terminal device of the client.

In an embodiment of the invention, the trusted third party updates the certificate database. The trusted third party is used to mean, e.g. a certificate authority (CA, Certificate Authority).

In an embodiment of the invention, the telecommunication network is used to mean a packet-switched network, e.g. an Internet network.

As compared to prior art the present invention provides several advantages. Thanks to the present invention, information proceeding in an open telecommunication network does not include the actual piece of information connected with the mode of debiting. This is used to mean that when the client pays his or her purchases with a credit card, the credit card number of the client is not sent over the telecommunication network at all. Due to this, the security level of the method presented by the invention is remarkably high.

Furthermore, the present invention is in no way restricted to a certain payment mode or payment system. It can be used in all payment modes.

Thanks to the present invention, the parties of a payment transaction do not need to make big investments in hardware or software improving the security.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following section, the invention will be described in detail by the aid of a few examples of its embodiments, in which

Fig. 1 represents one embodiment of the system in accordance with the invention,

Fig. 2 represents one embodiment of the system in accordance with the invention,

Fig. 3 represents one signaling flow chart in accordance with the invention, and

Fig. 4 represents one signaling flow chart in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

The system as shown in Fig. 1 comprises payment service equipment PS. Connected to the payment service equipment are five different databases: a client database DB, a service provider database RET, a transaction database TRANS, a verification database BL and a certificate database CERT. The client database DB comprises information relating to the clients. Client information may include, e.g. the name of the client, address, identity number, mobile number and the piece of information connected with the client's payment cards. The service provider database RET comprises information about registered service providers. The information relating to the service providers may include, e.g. the IP address of the service provider (IP, Internet Protocol). Further, the information relating to service providers may include, e.g. the payment cards accepted by the service provider and the bankers of the service provider.

To the transaction database TRANS, vouchers of the orders of products or services made via the payment service equipment PS are stored. The responsibility of the transaction database TRANS is to act as a kind of a voucher storage which enables one to afterwards unambiguously verify the purchases made, if necessary. The responsibility of the verification database BL is to save information about suspicious payment cards, thus acting as a kind of a black list. The

certificate database CERT comprises certificates generated to the clients that include, e.g. information relating to the clients and information relating to the issuer of the certificate. This kind of information may include, e.g. the name of the client and identity number, the address of the client, the public key of the client and the electronic identity. The certificate is issued by the trusted third party TTP, which also updates the certificate database CERT. The trusted third party TTP is advantageously used to mean a certificate authority.

The example as shown in Fig 1 comprises four access interfaces: a first access interface 1 to the payment system BANK, a second access interface 2 to the authentication system AUT, a third access interface 3 to the telecommunication network NET and a fourth access interface to the mobile communication network PLMN. The aforementioned systems, the database and the networks are connected to the payment service equipment PS via the relevant access interfaces. The mobile communication network PLMN is advantageously used to mean a mobile communication network consistent with the GSM system. The telecommunication network NET is primarily used to mean a packet-switched data transmission network, e.g. the Internet. The telecommunication network NET may, however, be any other packet-switched data transmission network.

The payment service equipment PS further comprises a generation block PAY for generating the billing ticket connected with the payment transaction. The telecommunication block PB is used to send and receive the confirmation of order connected with the billing ticket. The identification block ID is used to identify the client based on the electronic identity and/or signature. The information retrieval block IR is used to find out the payment card information relating to the client.

Connected to the mobile communication network PLMN is the payment terminal device PTE which is advantageously used to mean a mobile station. Connected to the mobile station PTE is the smart card SIM which is advantageously a subscriber identity module. Stored on the subscriber identity module SIM are, e.g. the electronic identity associated with the holder of the subscriber identity module SIM, the holder's private key and the public key associated with the payment service equipment. The private key is advantageously used to refer to the private key consistent with the PKI system.

Connected to the network NET are the service provider SP and the display terminal device DTE. The service provider SP is used to mean an entity which offers the clients a possibility of making purchases via the telecommunication network NET. The purchases are debited by means of the payment card of the client. The display terminal device DTE is advantageously used to mean an ordinary computer which comprises the necessary facilities and devices for using the service offered by the service provider PS.

Connected to the payment service equipment PS is an authentication system AUT. By means of the authentication system AUT, the payment service equipment PS may check the validity of the client'ts payment cards. In this example, the authentication system AUT consists of relevant data transmission networks. Via each data transmission network, the payment service equipment PS has the access to information systems of each company offering a payment card.

Connected to the payment service equipment PS is also a payment system BANK. The payment system BANK is generally used to mean a system which actually debits the client's payment card and correspondingly credits the account of the service provider SP with the same sum.

The payment service equipment PS may, when required, be separated from the telecommunication network NET by using a firewall. The firewall is used to mean a software or hardware configuration which is used to try to prevent the unauthorized access of extraneous entities to the resources of some company or to the ones of one´s own telecommunication network.

The system as shown in Fig. 2 comprises payment service equipment PS. Connected to the payment service equipment are five different databases: a client database DB, a service provider database RET, a transaction database TRANS, a verification database BL and a certificate database CERT. The client database DB comprises information relating to the clients. Client information may include, e.g. the name of the client, address, identity number, mobile number and the piece of information connected with the client´s payment cards. The service provider database RET comprises information about registered service providers. The information relating to the service providers may include, e.g. the IP address of the service provider (IP, Internet Protocol). Further, the information relating to service providers may include, e.g. the payment cards accepted by the service provider and the bankers of the service provider. To the transaction database TRANS, vouchers of the orders of products or services made via the payment service equipment PS are stored. The responsibility of the transaction database TRANS is to act as a kind of a voucher storage which enables one to afterwards unambiguously verify the purchases made, if necessary. The responsibility of the verification database BL is to save information about suspicious payment cards, thus acting as a kind of a black list. The certificate database CERT comprises certificates generated to the clients that include, e.g. information relating to the clients and information relating to the issuer of the certificate.

This kind of information may include, e.g. the name of the client and identity number, the address of the client, the public key of the client and the electronic identity. The certificate is issued by the trusted third party TTP, which also updates the certificate database CERT. The trusted third party TTP is advantageously used to mean a certificate authority.

In the example as shown in Fig. 2 the payment service equipment comprises three access interfaces: a first access interface 1 to the payment system BANK, a second access interface 2 to the authentication system AUT and a third access interface 3 to the telecommunication network NET. The aforementioned systems and the telecommunication network NET are connected to the payment service equipment PS via the relevant access interfaces. The telecommunication network NET is primarily used to mean a packet-switched data transmission network, e.g. the Internet. The telecommunication network NET may, however, be any other packet-switched data transmission network.

The payment service equipment PS further comprises a generation block PAY for generating the billing ticket connected with the payment transaction. The telecommunication block PB is used to send and receive the confirmation of order connected with the billing ticket. The identification block ID is used to identify the client based on the electronic identity and/or signature. The information retrieval block IR is used to find out the payment card information connected with the client.

Connected to the telecommunication network NET are the service provider SP and the terminal device TE. The service provider SP is used to mean an entity which offers the clients a possibility of making purchases via the telecommunication network NET . The purchases are debited from the payment card of the client. The terminal device TE is advantageously used

to mean an ordinary computer which comprises the necessary facilities and devices for using the service offered by the service provider SP. Connected to the terminal device TE is a smart card reader SCR. Into the card reader SCR, the smart card of the client may be input. Stored on the smart card SC are, e.g. the electronic identity associated with the holder of the smart card SC, the private key of the holder and the public key connected with the payment service equipment. The private key is preferably used to refer to the private key consistent with the PKI system. The card reader SCR may also be used to mean a facility internally installed in the terminal device TE

Connected to the payment service equipment PS is an authentication system AUT. By means of the authentication system AUT, the payment service equipment PS may check the validity of the client´s payment cards. In this example, the authentication system AUT consists of relevant data transmission networks. Via each data transmission network, the payment service equipment PS has the access to the information system of each company offering a payment card.

Connected to the payment service equipment PS is also a payment system BANK. The payment system BANK is generally used to mean a system which actually debits the client´s payment card and correspondingly credits the account of the service provider SP with the same sum.

The payment service equipment PS may, when required, be separated from the telecommunication network NET by using a firewall. The firewall is used to mean a software or hardware configuration which is used to try to prevent the unauthorized access of extraneous entities to the resources of some company or system.

Fig. 3 is one advantageous flow chart illustrating the function of the present invention. The ex-

ample as shown in Fig. 3 comprises a display device DTE, a payment terminal device PTE, a smart card SIM inserted into the payment terminal device PTE, a service provider SP, payment service equipment PS, a certificate database CERT, an authentication system AUT and a payment system BANK. The display terminal device DTE is advantageously used to mean an ordinary computer. The payment terminal device PTE is advantageously used to mean a mobile station and the smart card SIM the subscriber identity module of the mobile station.

The rhomb 30 is used to describe the actions the client takes via the computer DTE. The client chooses the www site connected with the service offered by the service provider SP. The service provided by the service provider may require a registration. In conjunction with the registering to the service the client transmits information about himself/herself to the service provider SP. The information may include, e.g. a name, address and mobile number. The access to the www sites required by the service may require that the client inputs a client identifier and a password. In addition, the client has got a certificate issued by a trusted third party. The certificate has been saved, e.g. to the certificate database of the payment service equipment PS. The payment service equipment PS comprises, for instance, a database which comprises all the service providers who have made a contract about the use of the payment service equipment PS. The service provider database includes, e.g. information about the payment cards accepted by the service provider and about the bankers of the service provider. The information included in the service provider database may be encrypted, e.g. with the public key of the payment service equipment, if required.

The arrow 31 is used to describe the information which the client transmits to the service pro-

vider SP via the www site. This is used to mean that the client has chosen the desired products and/or services via the www site of the service provider SP. In addition, he or she chooses the desired payment mode, which in this example is a Visa card. The client may be requested to fill in also his or her mobile number on the form. When all the necessary information has been filled in/chosen, the client sends the order, e.g. by pushing the pay button on the www site. As a consequence of pushing the pay button, the client may be displayed the www site produced by the payment service equipment.

The service provider SP sends the information received from the client to the payment service equipment PS, arrow 32. The service provider SP may send to the payment service equipment PS also information which the user himself/herself has not input into the www site. This kind of information may be, e.g. the mobile number included in the registration information of the client, the name or identifier of the service provider SP, the total sum of the products or services ordered and the date. The information sent by the service provider SP to the payment service equipment PS may be encrypted, if required, or a check sum may be computed at it using, e.g. a hash function. The Hash function is used to mean a function which generates an individual check sum from a given input. This enables one to make sure of the integrity of the information transferred. The generation of an encryption or check sum is, however, not necessary because the information sent by the service provider SP is not sensitive in itself. Let it be mentioned that the service provider SP does not at any point send to the payment service equipment PS more detailed information relating to the payment card of the client, e.g. the number of the payment card or its validity. As concerns the payment card of the client, the service pro-

vider SP may send to the payment service equipment PS only the piece of information concerning the payment card company, i.e. that the payment card is, e.g. Visa, MasterCard, Diners Club or a bank card.

The payment service equipment PS sends the confirmation of order to the mobile station PTE of the client, e.g. as a short message based on the information received from the service provider SP, arrow 33a. The confirmation of order includes information relating to the order made by the client. This kind of information is, e.g. the date, the products and services ordered, the total sum etc. The client checks the information of the confirmation of order. If the information included in the confirmation of order is correct, the client signs the confirmation of order with his or her own private signing key. It is possible to store to the subscriber identity module SIM the electronic identity associated with the holder and the private key of the holder. The private key is advantageously used to refer to the private key consistent with the PKI system. The signing with the mobile station may require that the client inputs into his or her mobile station a predetermined code, e.g. a PIN code (PIN, Personal Identification Number).

In addition to the confirmation of order, the client sends to the payment service equipment his or her own electronic identity from his or her mobile station PTE, arrow 33b. The payment service equipment PS receives the information sent from the mobile station PTE and checks the signature of the client in the certificate database CERT connected to the payment service equipment PS, arrows 34a and 34b. The right to read the certificate database CERT belongs solely to the payment service equipment PS. The payment service equipment PS further authenticates the client's signature and electronic identity, e.g. by utilizing the client database.

When the clien´ts identity has been verified, the payment service equipment PS finds out the credit card number of the client. This functionality is described by rhomb 35. The payment card number is checked, e.g. in the client database attached to the payment service equipment PS. The information included in the client database has been encrypted with the public key of the payment service equipment PS. In this way, only the payment service equipment PS can decode the information included in the client database into a readable form with its own private key. The client´s payment card number may alternatively be saved to the client-specific certificate of the certificate database CERT.

When the payment service equipment PS has found the client´s payment card number, it is sent to the authentication system AUT to be checked, arrow 36a. The authentication system AUT checks that the card indicated by the payment card number is valid. The authentication system AUT returns the result of the validity checking back to the payment service equipment PS, arrow 36b.

The payment connected with the order made by the client may now be effected. Prior to accepting the payment, it is possible to check in the verification database attached to the payment service equipment PS that the client´s payment card is not among suspicious or forbidden cards. The payment service equipment PS sends a confirmation of the effecting of the payment both to the service provider SP and to the client, arrows 37a and 37b. The command to effect the payment may now be sent to the payment system BANK, arrow 38. The payment system BANK debits the client´s payment card with the sum shown by the order and correspondingly credits the account of the service provider SP with the same sum.

Vouchers of all the orders made may be stored to the transaction database attached to the payment service equipment PS. The data record to be stored to the database includes, e.g. the following information:

- the electronic identity information of the client, the payment card details, account number, name and address,
- total sum of the order,
- recipient,
- date
- client's signature,
- authentication code,
- time stamp which has been received from a certificate authority.

In an embodiment as shown in Fig.3, the payment service equipment PS may comprise a functionality that the use of a certain payment card requires the use of a certain mobile number. This is used to mean that if the client wishes to pay his or her purchases, e.g. with a VISA card, he or she has to have a certain subscriber identity module SIM inserted into his or her mobile station.

In an embodiment as shown in Fig. 3, both the payment terminal device PTE and the display device DTE are used to mean physically the same device, preferably a mobile station.

Fig. 4 is one advantageous signaling flow chart illustrating the function of the present invention. The example as shown in Fig. 4 comprises a terminal device TE, a card reader SRC attached to the terminal device and a smart card SC compatible with it, a service provider SP, payment service equipment PS, a certificate database CERT, an authentication system AUT and a payment system BANK. The terminal device TE is advantageously used to mean a computer.

The rhomb 40 is used to describe the actions the client takes via the computer TE. The client

chooses the www site connected with the service offered by the service provider SP. The service provided by the service provider may require a registration. In conjunction with the registering to the service the client transmits information about himself/herself to the service provider SP. This kind of information may include, e.g. a name, address and mobile number. The access to the www sites required by the service may require that the client inputs a client identifier and a password. In addition, the client has got a certificate issued by a trusted third party. The certificate has been saved, e.g. to the certificate database of the payment service equipment PS. The payment service equipment PS comprises, for instance, a database which comprises all the service providers who have made a contract about the use of the payment service equipment PS. The service provider database includes, e.g. information about the payment cards accepted by the service provider and about the bankers of the service provider. The information included in the service provider database may be encrypted, e.g. with the public key of the payment service equipment, if required.

The arrow 41 is used to describe the information which the client transmits to the service provider SP via the www site. This is used to mean that the client has chosen the desired products and/or services via the www site of the service provider SP. In addition, he or she chooses the desired payment mode, which in this example is a Visa card. The client may be requested to fill in also his or her mobile number on the form. When all the necessary information has been filled in/chosen, the client sends the order, e.g. by pushing the pay button on the www site. As a consequence of pushing the pay button, the client may be displayed the www site produced by the payment service equipment.

The service provider SP sends the information received from the client to the payment service equipment PS, arrow 42. The service provider SP may send to the payment service equipment PS also information which the user himself/herself has not input into the www site. This kind of information may be, e.g. the mobile number included in the registration information of the client, the name or identifier of the service provider SP, the total sum of the products or services ordered and the date. The information sent by the service provider SP to the payment service equipment PS may be encrypted, if required, or a check sum may be computed at it using, e.g. a hash function. The Hash function is used to mean a function which generates an individual check sum from a given input. This enables one to make sure of the integrity of the information transferred. The generation of an encryption or check sum is, however, not necessary because the information sent by the service provider SP is not sensitive in itself. Let it be mentioned that the service provider SP does not at any point send to the payment service equipment PS more detailed information relating to the payment card of the client, e.g. the number of the payment card or its validity. As concerns the payment card of the client, the service provider SP may send to the payment service equipment PS only the piece of information concerning the payment card company, i.e. that the payment card is, e.g. Visa, MasterCard, Diners Club or a bank card.

The payment service equipment PS sends the confirmation of order to the terminal device TE of the client based on the information received from the service provider SP, arrow 43a. The confirmation of order includes information relating to the order made by the client. This kind of information is, e.g. the date, the products and services ordered, the total sum etc. The client checks the information of the confir-

mation of order. If the information included in the confirmation of order is correct, the client signs the confirmation of order with his or her own private signing key. The signature is carried out by means of a card reader SCR attached to the computer TE and by means of a client's smart card compatible with it. Stored on the smart card SC are the electronic identity associated with the holder of the smart card SC and the private key of the holder. The private key is advantageously used to refer to the private key consistent with the PKI system. The signing by means of the terminal device TE and the card reader SCR may require that the client inputs into his or her mobile station a predetermined code, e.g. a PIN code (PIN, Personal Identification Number).

In addition to the confirmation of order, the client sends to the payment service equipment PS his or her own electronic identity from his or her mobile station PTE, arrow 43b. The payment service equipment PS receives the information sent by the computer TE and checks the signature of the client in the certificate database CERT attached to the payment service equipment PS, arrows 44a and 44b. The right to read the certificate database CERT belongs solely to the payment service equipment PS. The payment service equipment PS further authenticates the client's signature and electronic identity, e.g. by utilizing the client database.

When the client's identity has been verified, the payment service equipment PS finds out the credit card number of the client. This functionality is described by rhomb 45. The payment card number is checked, e.g. in the client database attached to the payment service equipment PS. The information included in the client database has been encrypted with the public key of the payment service equipment PS. In this way, only the payment service equipment PS can

decode the information included in the client database into a readable form with its own private key. The client's payment card number may alternatively be saved to the client-specific certificate of the certificate database CERT.

When the payment service equipment PS has found the client's payment card number, it is sent to the authentication system AUT to be checked, arrow 46a. The authentication system AUT checks that the card indicated by the payment card number is valid. The authentication system AUT returns the result of the validity checking back to the payment service equipment PS, arrow 46b.

The payment connected with the order made by the client may now be effected. Prior to accepting the payment, it is possible to check in the verification database attached to the payment service equipment PS that the client's payment card is not among suspicious or forbidden cards. The payment service equipment PS sends a confirmation of the effecting of the payment both to the service provider SP and to the client, arrows 47a and 47b. The command to effect the payment may now be sent to the payment system BANK, arrow 48. The payment system BANK debits the client's payment card with the sum shown by the order and correspondingly credits the account of the service provider SP with the same sum.

Vouchers of all the orders made may be stored to the transaction database attached to the payment service equipment PS. The data record to be stored to the database includes, e.g. the following information:

- the electronic identity information of the client, the payment card details, account number, name and address,
- total sum of the order,
- recipient,
- date

- client's signature,
- authentication code,
- time stamp which has been received from a certificate authority.

The invention is not restricted merely to the embodiments referred to above, instead many variations are possible within the scope of the inventive idea defined by the claims.

CLAIMS

1. Payment service equipment comprising:

a first access interface (1) to the payment system (BANK);

a second access interface (2) to the authentication system (AUT);

a third access interface (3) to the telecommunication network (NET);

a certificate database (CERT) for storing the certificates associated with the clients;

a service provider database (RET) for storing the information relating to the registered service providers;

a client database (DB)for storing the information relating to the clients;

a transaction database (TRANS) for storing the information relating to the payment transactions;

a verification database (BL) which comprises an auxiliary list of suspicious payment cards,

characterised in that the payment service equipment comprises:

a generation block (PAY) for generating the billing ticket connected with the payment transaction;

a telecommunication block (PB) for sending and receiving the confirmation of order connected with the billing ticket;

an identification block (ID) for identifying the client based on the electronic identity and signature; and

an information retrieval block (IP) for finding out the payment card information of the client.

2. Payment service equipment as defined in claim 1, characterised in that the client information included in the client database (DB) comprises the client´s mobile number and/or information relating to the payment card of the client.

3. Payment service equipment as defined in claim 1 or 2, characterised in that the payment card is a credit card.

4. Payment service equipment as defined in any one of the preceding claims 1, 2 or 3, characterised in that the information included in the client database (DB) and/or in the service provider database (RET) is encrypted.

5. Payment service equipment as defined in any one of the preceding claims 1, 2, 3 or 4, characterised in that the payment card information is included in the certificate of the client in the certification database (CERT).

6. Payment service equipment as defined in any one of the preceding claims 1, 2, 3, 4 or 5, characterised in that the payment service equipment comprises a fourth access interface (4) to the mobile communication network.

7. A method for secure paying in a telecommunication system comprising:

a mobile communication network (PLMN);

a telecommunication network (NET);

a payment terminal device (PTE) which comprises a smart card (SIM) and which is connected to the mobile communication network (PLMN);

a display terminal device (DTE) which is connected to the mobile communication network (PLMN) and/or to the telecommunication network (NET);

a trusted third party (TTP);

a payment system (BANK);

a service provider (SP);

an authentication system (AUT);

which method comprises the steps of:

generating and issuing by the trusted third party (TTP) the certificate associated with the client;

choosing the product or service to be ordered by means of the display terminal device (DTE) from the

service provider (SP) via the telecommunication network (NET) and/or the mobile communication network (PLMN);

using the client's payment card and/or payment card information for the paying of the product or service ordered;

characterised in that the method further comprises the steps of:

generating by means of the payment service equipment the billing ticket connected with the product or service ordered;

sending a confirmation of order to the payment terminal device (PTE) of the client via the mobile communication network (PLMN);

signing and/or encrypting the aforementioned confirmation of order by means of the payment terminal device (PTE);

sending the aforementioned signed and/or encrypted confirmation of order and the electronic identity information associated with the client from the payment terminal device (PTE) to the payment service equipment (PS) by way of the mobile communication network (PLMN);

identifying the client by the payment service equipment (PS) based on the aforementioned signature and/or electronic identity information;

retrieving the payment card number associated with the client based on the aforementioned signature and/or electronic identity information.

checking the use of right of the payment card and accepting the payment, if the payment card was successfully verified.

8. A method as defined in claim 7, characterised in that the client is identified based on the information included in the certificate database (CERT).

9. A method as defined in claim 7 or 8, characterised in that the payment card number associated with the client is retrieved from the client database (DB) of the payment service equipment (PS).

10. A method as defined in claim 7 or 8, characterised in that the payment card number of the client is retrieved from the certificate database (CERT) attached to the payment service equipment (PS).

11. A method as defined in any one of the preceding claims 7, 8, 9 or 10, characterised in that the validity of the payment card is checked in the authentication system (AUT).

12. A method as defined in any one of the preceding claims 7, 8, 9, 10 or 11, characterised in that one checks in the verification database (BL) that the payment card is not among suspicious or forbidden cards.

13. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11 or 12, characterised in that the request for the debiting of the payment is sent to the payment system (BANK) after the validity of the payment card has been checked.

14. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12 or 13, characterised in that the confirmation of the succeeding of the order is sent to the client's display terminal device (DTE) or payment terminal device (PTE) and to the service provider (SP).

15. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13 or 14, characterised in that the certificate database is updated by the trusted third party (TTP).

16. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14 or 15, characterised in that the payment terminal

device (PTE) and the display terminal device (DTE) are used to mean a mobile station.

17. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15 or 16, characterised in that the payment terminal device (PTE) is used to mean a mobile station and the display terminal device (DTE) a computer.

18. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 or 17, characterised in that the payment card is used to mean a Visa, MasterCard or Diners Club card or a bank card.

19. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17 or 18, characterised in that the smart card (SIM) is used to mean a subscriber identity module.

20. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 or 19, characterised in that stored on the smart card (SIM) are the electronic identity of the client and the client's private key.

21. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 or 20, characterised in that stored on the smart card (SIM) is the public key associated with the payment service equipment (PS).

22. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 or 21, characterised in that the mobile communication network (PLMN) is used to mean a mobile communication network consistent with the GSM system.

23. A method as defined in any one of the preceding claims 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 or 22, characterised in that the telecommunication network (NET) is used to

mean a packet-switched network, e.g. the Internet network.

24. A method for secure paying in a telecommunication network comprising:

a telecommunication network (NET);

a terminal device (TE) to which terminal device there is a card reader (SCR) attached and into which card reader it is possible to input a smart card (SC) and which terminal device (TE) is connected to the telecommunication network (NET);

a trusted third party (TTP);

a payment system (BANK);

a service provider (SP);

an authentication system (AUT);

which method comprises the steps of:

generating and issuing by the trusted third party (TTP) the certificate associated with the client;

choosing the product or service to be ordered by means of the terminal device (TE) from the service provider (SP) via the telecommunication network (NET);

using the client's payment card and/or payment card information for the paying of the product or service ordered;

characterised in that the method further comprises the steps of:

generating by means of the payment service equipment (PS) the billing ticket connected with the product or service ordered;

sending a confirmation of order to the terminal device (TE) of the client via the telecommunication network (NET);

signing and/or encrypting the aforementioned confirmation of order with the terminal device (TE) by means of a card reader (SCR) attached to it and by means of a smart card (SC) inserted into the card reader;

sending the aforementioned signed and/or encrypted confirmation of order and the electronic identity in-

formation associated with the client from the terminal device (TE) to the payment service equipment (PS) by way of the telecommunication network (NET);

identifying the client by the payment service equipment (PS) based on the aforementioned signature and/or electronic identity information;

retrieving the payment card number associated with the client based on the aforementioned signature and/or electronic identity information.

checking the use of right of the payment card and accepting the payment, if the payment card was successfully verified.

25. A method as defined in claim 24, characterised in that the client is identified based on the information included in the certification database (CERT).

26. A method as defined in claim 24 or 25, characterised in that the payment card number associated with the client is retrieved from the database (DB) of the payment service equipment (PS).

27. A method as defined in claim 24 or 25, characterised in that the payment card number of the client is retrieved from the certificate database (CERT) attached to the payment service equipment (PS).

28. A method as defined in any one of the preceding claims 24, 25, 26 or 27, characterised in that the validity of the payment card is checked in the authentication system (AUT).

29. A method as defined in any one of the preceding claims 24, 25, 26, 27 or 28, characterised in that one checks in the verification database (BL) that the payment card is not among suspicious or forbidden cards.

30. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28 or 29, characterised in that the request for the debiting

of the payment is sent to the payment system (BANK) after the validity of the payment card has been checked.

31. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29 or 30, characterised in that a confirmation of the succeeding of the order is sent to the terminal device (TE) of the client and to the service provider (SP).

32. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30 or 31, characterised in that the certificate database is updated by the trusted third party (TTP).

33. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30, 31 or 32, characterised in that the terminal device (TE) is used to mean a computer.

34. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30, 31, 32 or 33, characterised in that the payment card is used to mean a Visa, MasterCard or Diners Club card or a bank card.

35. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 or 34, characterised in that stored on the smart card (SC) are the client's electronic identity and private key.

36. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34 or 35, characterised in that stored on the smart card (SC) is the public key associated with the payment service equipment (PS).

37. A method as defined in any one of the preceding claims 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35 or 36, characterised in that the telecommunication network (NET) is used to mean a packet-switched network, e.g. the Internet network.

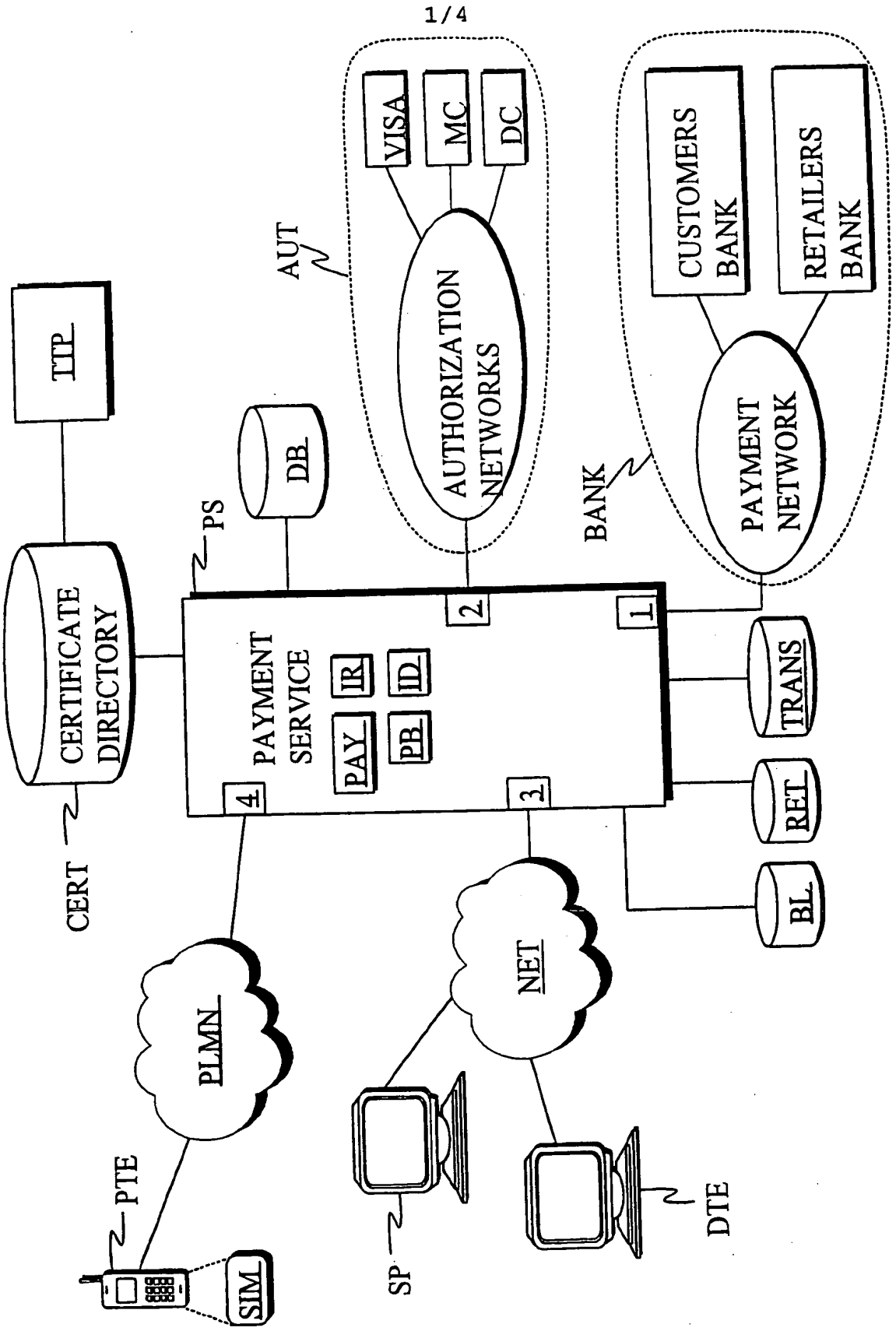

TTP
CERTIFICATE DIRECTORY
CERT
PS
DB
AUT
VISA
MC
DC
AUTHORIZATION NETWORKS
BANK
CUSTOMERS BANK
RETAILERS BANK
PAYMENT NETWORK
PAYMENT SERVICE
IR
ID
PAY
PB
1
2
3
4
TRANS
RET
BL
PLMN
NET
PTE
SIM
SP
DTE

Fig. 1

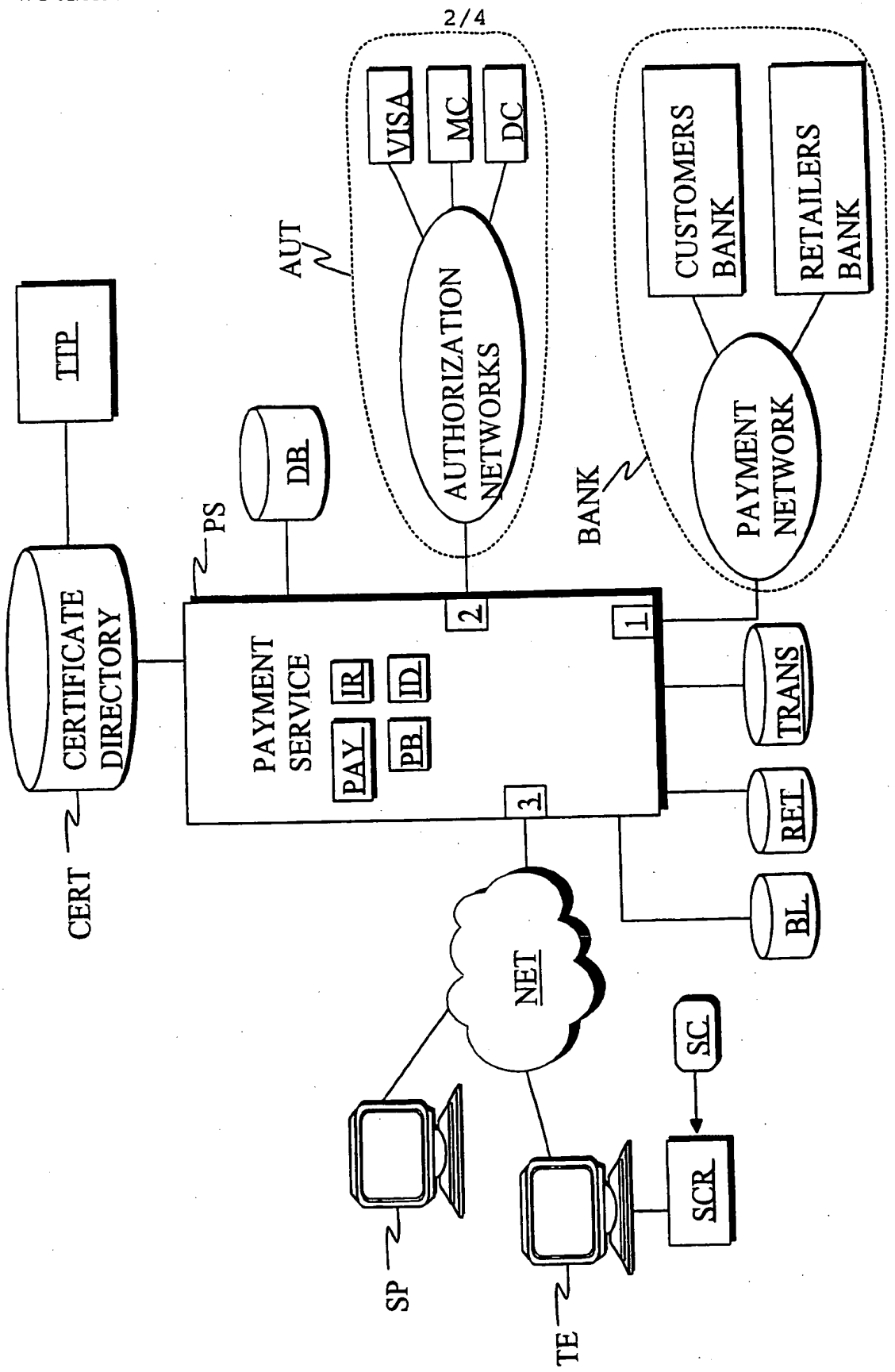

TTP
CERTIFICATE DIRECTORY
CERT
PS
DB
PAYMENT SERVICE
IR
ID
PAY
PB
2
1
3
AUT
VISA
MC
DC
AUTHORIZATION NETWORKS
BANK
CUSTOMERS BANK
RETAILERS BANK
PAYMENT NETWORK
TRANS
RET
BL
NET
SC
SCR
SP
TE

Fig. 2

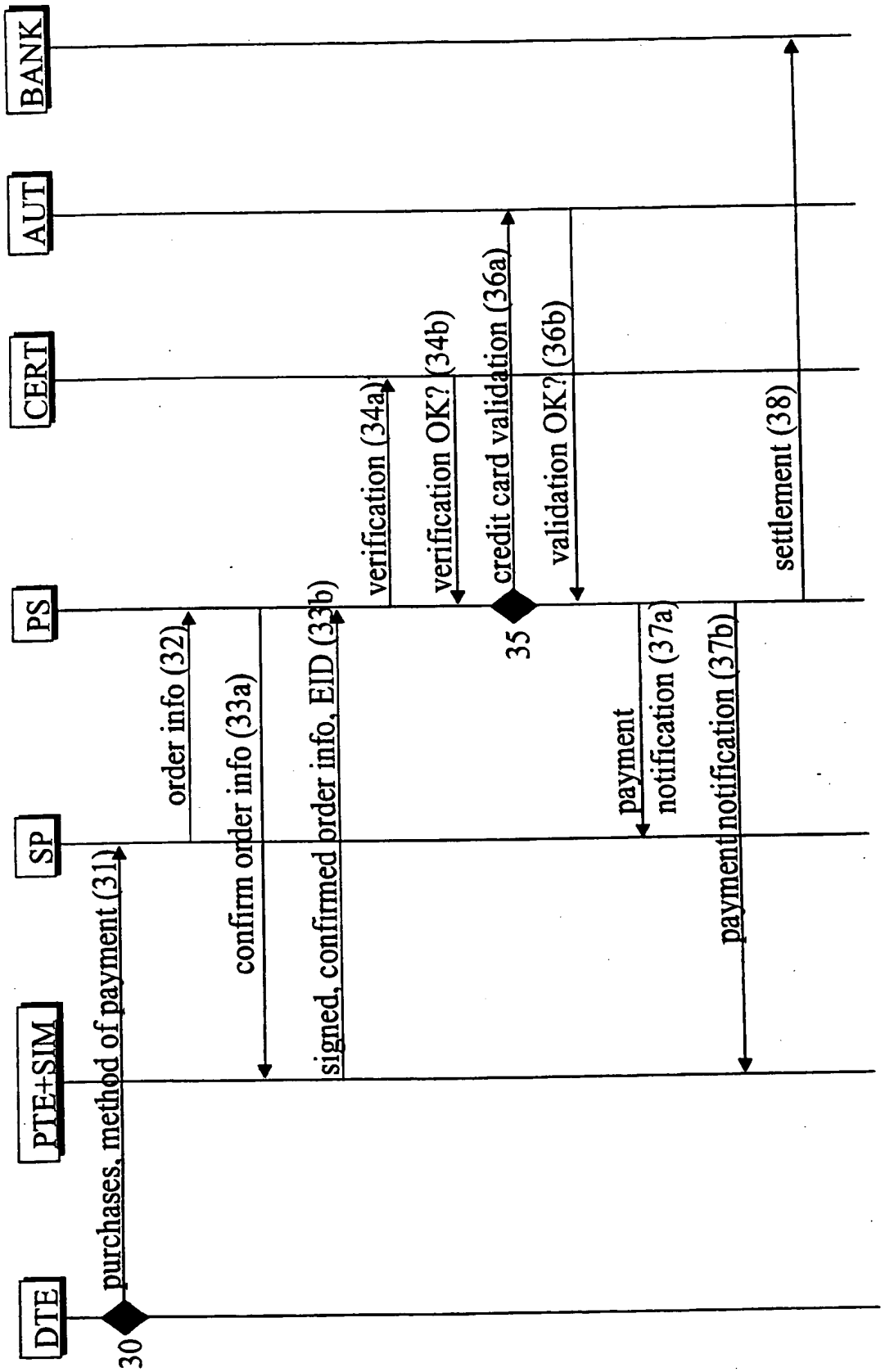

DTE
PTE+SIM
SP
PS
CERT
AUT
BANK
30
purchases, method of payment (31)
order info (32)
confirm order info (33a)
signed, confirmed order info, EID (33b)
verification (34a)
verification OK? (34b)
35
credit card validation (36a)
validation OK? (36b)
payment notification (37a)
payment notification (37b)
settlement (38)

Fig. 3

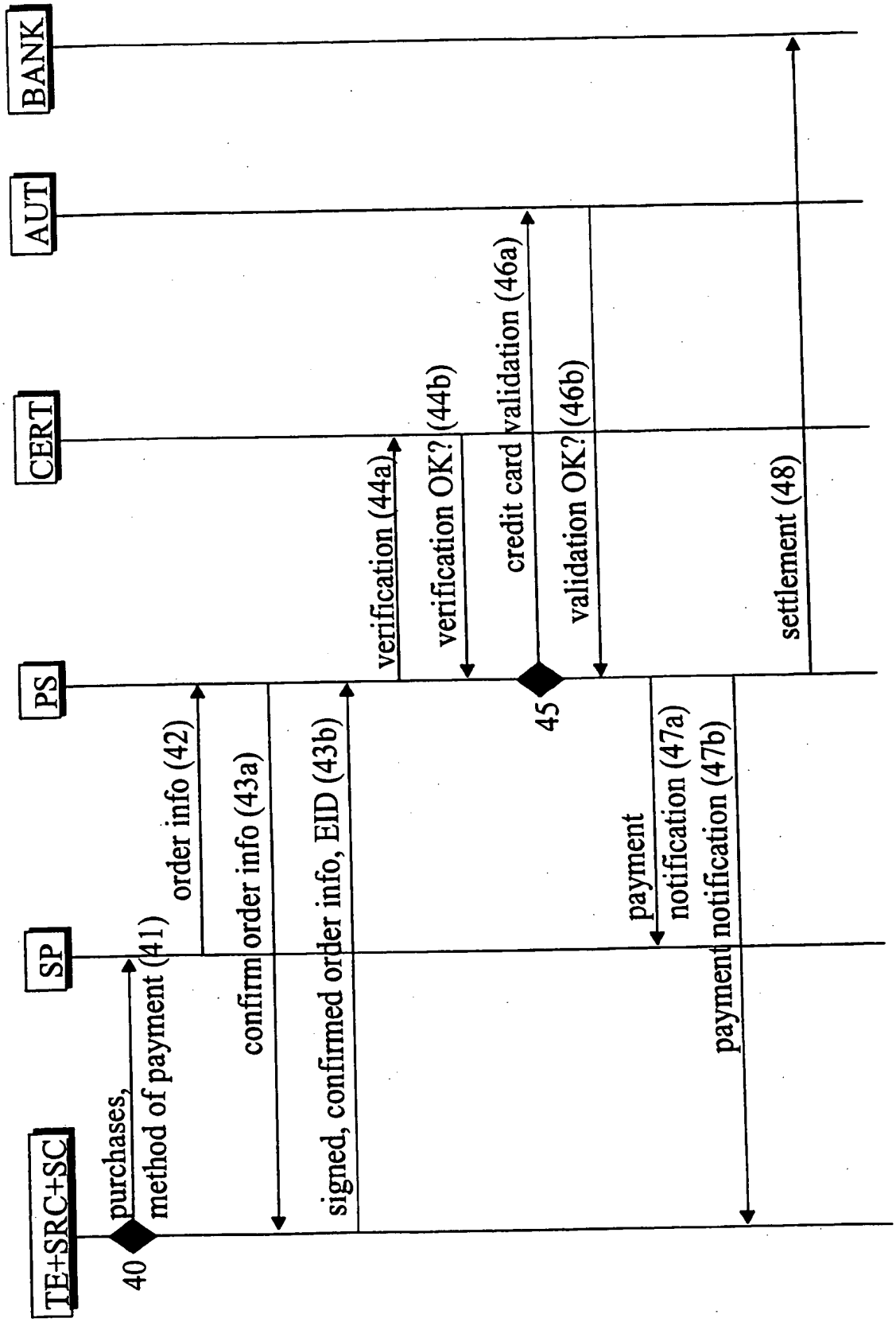

TE+SRC+SC
SP
PS
CERT
AUT
BANK
purchases, method of payment (41)
order info (42)
confirm order info (43a)
signed, confirmed order info, EID (43b)
verification (44a)
verification OK? (44b)
credit card validation (46a)
validation OK? (46b)
settlement (48)
payment notification (47a)
payment notification (47b)
40
45

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00063

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G07F 7/10 // G06F 17&60
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9516971 A1 (OPEN MARKET, INC.), 22 June 1995 (22.06.95), page 5, line 16 - line 28; page 14, line 6 - page 16, line 23; page 20, line 3 - line 22, figures 12-14 --	1,24
X	WO 9608783 A1 (FIRST VIRTUAL HOLDINGS, INC.), 21 March 1996 (21.03.96), page 5, line 25 - page 6, line 28; page 19, line 84 - page 21, line 16 --	1,24
A	WO 9964995 A1 (BARCLAYS BANK PLC), 16 December 1999 (16.12.99), page 2, line 8 - page 3, line 6 --	1-3,7-10, 24-27

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2001	14 June 2001 (14.06.01)
Name and mailing address of the ISA Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Inger Löfving / JA A Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00063

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9826386 A1 (MASCHOFF, KURT, M.), 18 June 1998 (18.06.98), page 4, line 18 - page 8, line 2	1-3,7-10, 24-27
	--	
A	WO 9847112 A1 (STRATEX/PARADIGM (UK) LIMITED), 22 October 1998 (22.10.98), whole document	1-3,7-10, 24-27
	--	
A	US 5991738 A (OGRAM), 23 November 1999 (23.11.99), whole document	1-3,7-10, 24-27
	--	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI01/00063

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 4-6,11-23,28-37
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/05/01

International application No.
PCT/FI 01/00063

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9516971 A1	22/06/95	EP 0734556 A	02/10/96
		JP 9500470 T	14/01/97
		JP 10312433 A	24/11/98
		JP 10312434 A	24/11/98
		JP 11096243 A	09/04/99
		US 5724424 A	03/03/98
		US 6049785 A	11/04/00
		US 6195649 B	27/02/01
		US 6199051 B	06/03/01
		US 6205437 B	20/03/01
WO 9608783 A1	21/03/96	AU 696475 B	10/09/98
		AU 3630995 A	29/03/96
		AU 9703898 A	18/02/99
		CA 2199942 A	21/03/96
		EP 0791202 A	27/08/97
		JP 10508708 T	25/08/98
		NZ 293783 A	28/10/98
		US 5826241 A	20/10/98
WO 9964995 A1	16/12/99	AU 9175798 A	30/12/99
		CN 1266520 T	13/09/00
		DE 29824106 U	13/07/00
		GB 2338381 A	15/12/99
		GB 9812520 D	00/00/00
WO 9826386 A1	18/06/98	AU 5382098 A	03/07/98
		EP 0961999 A	08/12/99
WO 9847112 A1	22/10/98	AU 7061098 A	11/11/98
		EP 1010148 A	21/06/00
US 5991738 A	23/11/99	US 5822737 A	13/10/98
		US 5963917 A	05/10/99